PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-203237
(43)Date of publication of application : 30.07.1999

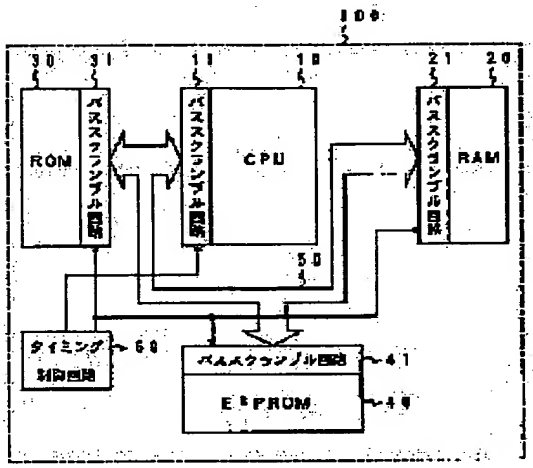
(51)Int.Cl. G06F 13/36
G06F 13/38
G06F 15/78
G06K 19/073

(21)Application number : 10-006509
(22)Date of filing : 16.01.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : HASEBE SHINICHI

(54) SEMICONDUCTOR INTEGRATED CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a new security system an IC internal part of which can not easily be analyzed.
SOLUTION: Order of an address and data outputted from a CPU 10 are changed regularly or in a random cycle by a bus scramble circuit 11. Thus, the address and the data outputted to each of plural bus lines 50 change hour to hour and cannot specify the meaning (kind) of the data given to a specified bus line. The address and the data of the bus line 50 have their order returned to the original order by the bus scramble circuits 21, 31 and 41 before they are inputted to memories 20, 30 and 40. A timing control circuit 60 changes the order of the address and the data and decides a cycle in which the order is returned to the original one.



LEGAL STATUS

[Date of request for examination] 15.06.2001
[Date of sending the examiner's decision of rejection] 03.06.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－203237

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	13/36	３２０	Ｇ０６Ｆ	13/36	３２０Ｚ
	13/38	３３０		13/38	３３０Ｚ
	15/78	５１０		15/78	５１０Ｇ
Ｇ０６Ｋ	19/073		Ｇ０６Ｋ	19/00	Ｐ

審査請求　未請求　請求項の数５　ＯＬ　（全５頁）

(21)出願番号　特願平10－6509

(22)出願日　平成10年(1998)１月16日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　長谷部　信一
神奈川県川崎市幸区堀川町580番１号　株式会社東芝半導体システム技術センター内

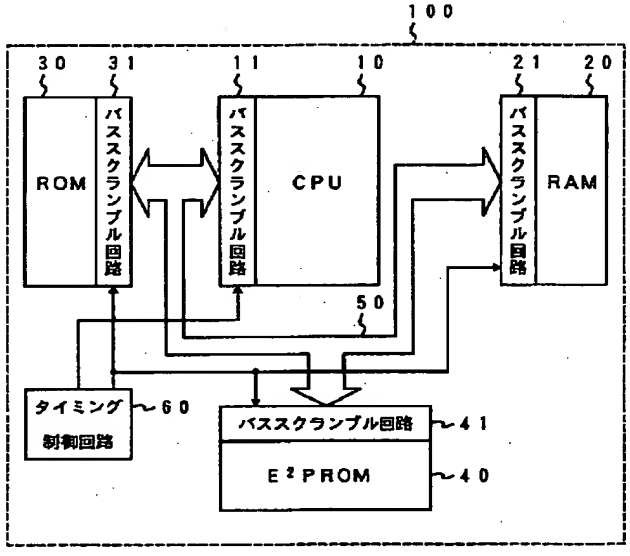
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　半導体集積回路

(57)【要約】

【課題】　ＩＣ内部を解析されない新規なセキュリティシステムを提供する。

【解決手段】　ＣＰＵ１０から出力されるアドレス及びデータの順序は、バススクランブル回路１１により、定期的又はランダムな周期で変えられる。このため、複数本のバスライン５０の各々に出力されるアドレス及びデータは、時々刻々と変化し、所定のバスラインに与えられるデータの意味（種類）を特定することはできない。バスライン５０のアドレス及びデータは、メモリ２０，３０，４０に入力される前に、バススクランブル回路２１，３１，４１により元の順序に戻される。タイミング制御回路６０は、アドレス及びデータの順序を変え、元に戻す周期を決定する。



【特許請求の範囲】
【請求項１】　複数ビットの信号を送信する第１ブロックと、前記複数ビットの信号を受信する第２ブロックと、前記複数ビットの信号を前記第１ブロックから前記第２ブロックへ転送する複数本のバスラインと、前記第１ブロックから出力される複数ビットの信号の順序を変えて前記複数本のバスラインに導く第１バススクランブル回路と、前記複数本のバスラインの複数ビットの信号の順序を元に戻して前記第２ブロックに導く第２バススクランブル回路とを具備することを特徴とする半導体集積回路。
【請求項２】　請求項１記載の半導体集積回路において、
さらに、前記第１ブロックから出力される複数ビットの信号の順序を定期的又はランダムな周期で変えるように前記第１バススクランブル回路を制御し、前記複数本のバスラインの複数ビットの信号の順序を定期的又はランダムな周期で元に戻すように前記第２バススクランブル回路を制御するタイミング制御回路を具備することを特徴とする半導体集積回路。
【請求項３】　前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第１ブロックから出力される複数ビットの信号のうちの所定の１ビットの値により決定することを特徴とする請求項２記載の半導体集積回路。
【請求項４】　前記第１ブロックは、ＣＰＵの機能を有し、前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第１ブロックから出力されるクロックの周期よりも長く設定されていることを特徴とする請求項２記載の半導体集積回路。
【請求項５】　前記第１ブロックは、ＣＰＵの機能を有し、前記第２ブロックは、メモリの機能を有し、前記複数ビットの信号は、前記メモリをアクセスするアドレス又は前記メモリに入力するデータを含んでいることを特徴とする請求項２記載の半導体集積回路。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣ（半導体集積回路）の内部を悪意のあるアタッカーに解析されないように、アドレスバス及びデータバスに出力するアドレス及びデータの順序をランダムに変えるセキュリティシステムに関する。
【０００２】
【従来の技術】従来、ＩＣカードなどのセキュリティの必要のある製品においては、ＩＣの内部を悪意のあるアタッカーに解析されないように、アドレスバス及びデータバスを物理的に混在させて、容易にＩＣの内部を解析できないようにしていた。
【０００３】しかし、このようなセキュリティシステムでは、ＩＣの製造段階（配線工程）において、マスクのパターンによりアドレスバス及びデータバスの配置（順序）が決定されてしまい、ＩＣの製造後に、アドレスバス及びデータバスの配置をランダムに変えることができない。
【０００４】このため、悪意のあるアタッカーがＩＣの内部を繰り返し解析すると、最後には、アドレスバス及びデータバスの配置が判明してしまい、ＩＣのセキュリティが十分に行われていなかった。
【０００５】
【発明が解決しようとする課題】このように、従来は、悪意のあるアタッカーがＩＣの内部を繰り返し解析すると、最後には、アドレスバス及びデータバスの配置が判明してしまい、ＩＣのセキュリティが十分に行われないという欠点がある。
【０００６】本発明は、上記欠点を解決すべくなされたもので、その目的は、悪意のあるアタッカーがＩＣの内部を繰り返し解析しても、アドレス及びデータを特定できないような新規なセキュリティシステムを提供することである。
【０００７】
【課題を解決するための手段】上記目的を達成するため、本発明の半導体集積回路は、複数ビットの信号を送信する第１ブロックと、前記複数ビットの信号を受信する第２ブロックと、前記複数ビットの信号を前記第１ブロックから前記第２ブロックへ転送する複数本のバスラインと、前記第１ブロックから出力される複数ビットの信号の順序を変えて前記複数本のバスラインに導く第１バススクランブル回路と、前記複数本のバスラインの複数ビットの信号の順序を元に戻して前記第２ブロックに導く第２バススクランブル回路とを備える。
【０００８】本発明の半導体集積回路は、さらに、前記第１ブロックから出力される複数ビットの信号の順序を定期的又はランダムな周期で変えるように前記第１バススクランブル回路を制御し、前記複数本のバスラインの複数ビットの信号の順序を定期的又はランダムな周期で元に戻すように前記第２バススクランブル回路を制御するタイミング制御回路を備える。
【０００９】前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第１ブロックから出力される複数ビットの信号のうちの所定の１ビットの値により決定する。
【００１０】前記第１ブロックがＣＰＵの機能を有している場合、前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第１ブロックから出力されるクロックの周期よりも長く設定される。
【００１１】前記第１ブロックがＣＰＵの機能を有し、前記第２ブロックがメモリの機能を有している場合、前記複数ビットの信号は、前記メモリをアクセスするアドレス又は前記メモリに入力するデータを含んでいる。
【００１２】

【発明の実施の形態】以下、図面を参照しながら、本発明の半導体集積回路について詳細に説明する。図１は、本発明に関わるバススクランブル回路を有するＩＣ（半導体集積回路）の内部構成の一例を示している。

【００１３】ＩＣ１００内は、複数のブロックから構成されており、例えば、複数のブロックには、ＣＰＵ（central processing unit ）１０、ＲＡＭ（random access memory）２０、ＲＯＭ（read only memory）３０、Ｅ^2 ＰＲＯＭ（electrically erasable programmable ROM）４０などが含まれている。

【００１４】各ブロック１０，２０，３０，４０のＩ／Ｏ部（データの入出力部）及びアドレスの入出力部には、これらに隣接する形でバススクランブル回路１１，２１，３１，４１が設けられている。また、各バススクランブル回路１１，２１，３１，４１を互いに接続するバスライン５０が配置されている。バスライン５０は、ｎ（例えば、１６）ビットのアドレスバス及びｍ（例えば、８）ビットのデータバスから構成されている。

【００１５】タイミング制御回路６０は、各ブロックに対応して設けられたバススクランブル回路の動作を制御する。タイミング制御回路６０は、例えば、図３に示すようなフリップフロップ回路から構成できる。この場合、ｎ＋ｍ本のバスラインに対して、フリップフロップ回路は、$\log_2$（ｎ＋ｍ）個必要となる。

【００１６】図２は、図１のバススクランブル回路の構成の一例を示すものである。但し、図２では、説明を簡単にするため、バスライン５０が２ビットのデータバスから構成されているものと仮定している。

【００１７】ＣＰＵ１０の入出力端子Ｉ／Ｏ・０は、バススクランブル回路１１のトランジスタＴ００を経由してデータバスＢＤ０に接続されると共に、バススクランブル回路１１のトランジスタＴ０１を経由してデータバスＢＤ１に接続される。また、ＣＰＵ１０の入出力端子Ｉ／Ｏ・１は、バススクランブル回路１１のトランジスタＴ１０を経由してデータバスＢＤ１に接続されると共に、バススクランブル回路１１のトランジスタＴ１１を経由してデータバスＢＤ０に接続される。

【００１８】ＲＡＭ２０の入出力端子Ｉ／Ｏ・０は、バススクランブル回路２１のトランジスタＴ００を経由してデータバスＢＤ０に接続されると共に、バススクランブル回路２１のトランジスタＴ０１を経由してデータバスＢＤ１に接続される。また、ＲＡＭ２０の入出力端子Ｉ／Ｏ・１は、バススクランブル回路２１のトランジスタＴ１０を経由してデータバスＢＤ１に接続されると共に、バススクランブル回路２１のトランジスタＴ１１を経由してデータバスＢＤ０に接続される。

【００１９】ＲＯＭ３０の入出力端子Ｉ／Ｏ・０は、バススクランブル回路３１のトランジスタＴ００を経由してデータバスＢＤ０に接続されると共に、バススクランブル回路３１のトランジスタＴ０１を経由してデータバスＢＤ１に接続される。また、ＲＯＭ３０の入出力端子Ｉ／Ｏ・１は、バススクランブル回路３１のトランジスタＴ１０を経由してデータバスＢＤ１に接続されると共に、バススクランブル回路３１のトランジスタＴ１１を経由してデータバスＢＤ０に接続される。

【００２０】Ｅ^2 ＰＲＯＭ４０の入出力端子Ｉ／Ｏ・０は、バススクランブル回路４１のトランジスタＴ００を経由してデータバスＢＤ０に接続されると共に、バススクランブル回路４１のトランジスタＴ０１を経由してデータバスＢＤ１に接続される。また、Ｅ^2 ＰＲＯＭ４０の入出力端子Ｉ／Ｏ・１は、バススクランブル回路４１のトランジスタＴ１０を経由してデータバスＢＤ１に接続されると共に、バススクランブル回路４１のトランジスタＴ１１を経由してデータバスＢＤ０に接続される。

【００２１】各バススクランブル回路１１，２１，３１，４１のトランジスタＴ００，Ｔ１０のゲートには、タイミング制御信号ϕが入力され、各バススクランブル回路１１，２１，３１，４１のトランジスタＴ０１，Ｔ１１のゲートには、タイミング制御信号／ϕが入力される。

【００２２】このような構成によれば、例えば、ＣＰＵ１０からＲＡＭ２０にデータを転送する場合を考えると、ＣＰＵ１０の入出力端子Ｉ／Ｏ・０から出力されるデータは、バスラインＢＤ０を経由してＲＡＭ２０の入出力端子Ｉ／Ｏ・０に到る経路とバスラインＢＤ１を経由してＲＡＭ２０の入出力端子Ｉ／Ｏ・０に到る経路の２通りの経路のうちのいずれも取り得ることがわかる。ＣＰＵ１０の入出力端子Ｉ／Ｏ・１から出力されるデータについても、同様である。

【００２３】つまり、タイミング制御信号ϕ，／ϕのレベルを適当な時期に切り替えることにより、例えば、ＣＰＵ１０の入出力端子Ｉ／Ｏ・０から出力されるデータは、バスラインＢＤ０を経由してＲＡＭ２０の入出力端子Ｉ／Ｏ・０に導かれたり、又はバスラインＢＤ１を経由してＲＡＭ２０の入出力端子Ｉ／Ｏ・０に導かれたりすることになる。

【００２４】このように、本発明によれば、バススクランブル回路により、データバスＢＤ０，ＢＤ１に出力されるデータの意味（又は種類）を時々刻々と変化させることができるため、悪意のアタッカーがＩＣ内を繰り返し解析しても、各バスラインのデータの意味（又は種類）を特定することができず、ＩＣのセキュリティが完璧となる。

【００２５】なお、タイミング制御信号ϕ，／ϕのレベルの切り替え（データ経路の切り替え）は、例えば、特定のブロック（例えば、ＣＰＵ）の特定の入出力端子Ｉ／Ｏ・ｊから出力されるデータに基づいて行うことができる。また、各ブロック間でデータの意味を取り違えないように、タイミング制御信号ϕ，／ϕのレベルの切り替えは、各ブロック間でのデータの授受が完了した後に

行われる。

【００２６】当然に、データ送信側のブロックのバススクランブル回路におけるタイミング制御信号φ，／φのレベルの切り替え時期とデータ受信側のブロックのバススクランブル回路におけるタイミング制御信号φ，／φのレベルの切り替え時期は、データの転送時間を考慮すれば、データの転送時間分だけずれることになる。

【００２７】タイミング制御信号φ，／φのレベルの切り替え周期は、例えば、ＣＰＵが生成するクロックＣＬＫの周期よりも十分に長くするのがよい。切り替え周期がクロックＣＬＫの周期と同等程度に短くなると、データの誤認識の発生する確率が高くなるからである。タイミング制御信号φ，／φのレベルの切り替え周期は、定期的であっても、ランダムであってもよい。

【００２８】図４は、本発明の原理を簡単に示すものである。例えば、ＣＰＵから出力されるアドレスがｎビット、データがｍビットであると仮定すると、バスライン１本で１ビットのデータ転送が可能であるから、アドレスバスとデータバスを合計した本数は、ｎ＋ｍ本となる。但し、本発明では、上述のように、各バスラインに出力されるアドレス及びデータは、時々刻々と変化するため、ｎ＋ｍ本の各バスラインの意味（種類）は特定されない。

【００２９】本例では、仮に、ｎ＋ｍ本のバスラインにそれぞれ符号ＢＡ０～ＢＡｎ，ＢＤ０～ＢＤｍを付すことにする。この場合、ｎ＋ｍビットの各データの信号経路の組み合わせは、ｎ＋ｍの階乗だけ存在する。よって、バススクランブル回路により、このｎ＋ｍの階乗だけ存在する信号経路を一定周期で又はランダムに変えてやれば、悪意のあるアタッカーにＩＣの内部が解析されることはない。

【００３０】表１は、ＣＰＵからアドレス２ビット、データ２ビットが出力されると仮定した場合において、アドレス及びデータの信号経路の組み合わせを全て羅列したものである。

【００３１】

【表１】

アドレス２ビット、データ２ビットの場合→２４通り

バスライン	データ											
BA0	A0	A0	A0	A0	A0	A0	A1	A1	A1	A1	A1	A1
BA1	A1	A1	D0	D0	D1	D1	A0	A0	D0	D0	D1	D1
BD0	D0	D1	A1	D1	A1	D0	D0	D1	A0	D1	A0	D0
BD1	D1	D0	D1	A1	D0	A1	D1	D0	D1	A0	D0	A0
バスライン	データ											
BA0	D0	D0	D0	D0	D0	D0	D1	D1	D1	D1	D1	D1
BA1	A0	A0	A1	A1	D1	D1	A0	A0	A1	A1	D0	D0
BD0	D1	A1	D1	A0	A0	A1	D0	A1	D0	A0	A0	A1
BD1	A1	D1	A0	D1	A1	A0	A1	D0	A0	D0	A1	A0

【００３２】つまり、アドレス及びデータの合計は４ビット、バスラインの数は４本であるから、４の階乗、即ち、２４通りの信号経路の組み合わせが考えられる。なお、アドレス及びデータの順序は、送信側のＣＰＵのバススクランブル回路によりランダムに変えられた後にバスラインに出力されるが、当然に、受信側のメモリのバススクランブル回路により正しい順序に戻されてメモリに与えられることになる。

【００３３】

【発明の効果】以上、説明したように、本発明のバススクランブル回路によれば、アドレス及びデータの順序を送信ブロック側でランダムに変えた後、バスラインに出力し、かつ、受信ブロック側で正しい順序に戻すような構成とし、アドレス及びデータの転送経路を時々刻々と変化させるようにしている。つまり、各バスラインに出力されるデータの意味（又は種類）が特定されないため、悪意のあるアタッカーがＩＣの内部を繰り返し解析しても、アドレス及びデータを特定できず、完璧なセキュリティシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明のバススクランブル回路を有するＩＣの構成の一例を示す図。

【図２】バススクランブル回路の構成の一例を示す図。

【図３】タイミング制御回路を構成するフリップフロップ回路を示す図。

【図４】本発明の原理を示す図。

【符号の説明】

１０　：ＣＰＵ、

１１，２１，３１，４１　：バススクランブル回路、

２０　：ＲＡＭ、

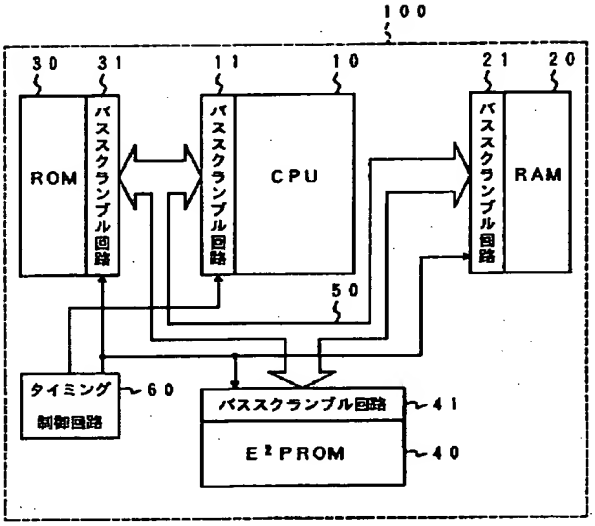
３０　：ＲＯＭ、

４０　：E^2 ＰＲＯＭ、

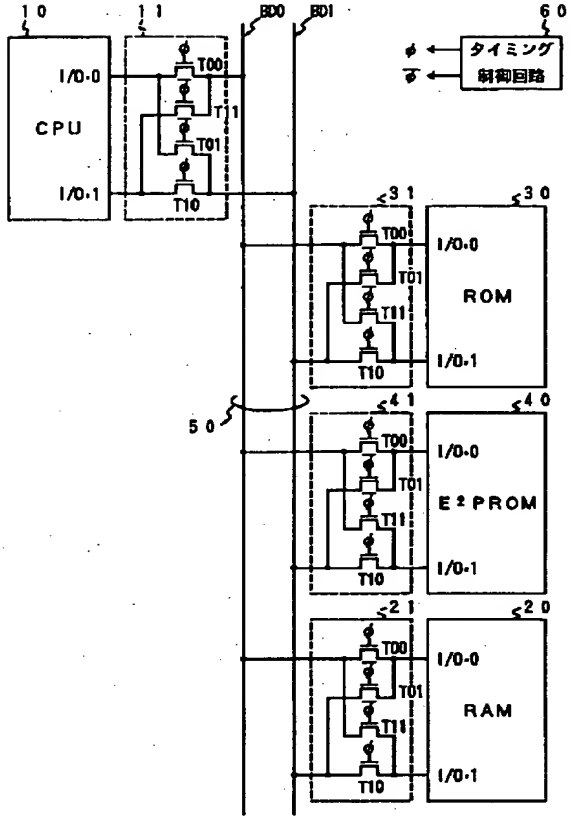
５０　：バスライン、

６０　：タイミング制御回路。

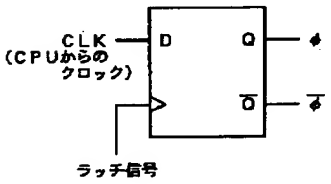
【図１】


100
30
31
11
10
21
20
ROM
バススクランブル回路
バススクランブル回路
CPU
バススクランブル回路
RAM
50
タイミング制御回路
60
バススクランブル回路
41
E²PROM
40

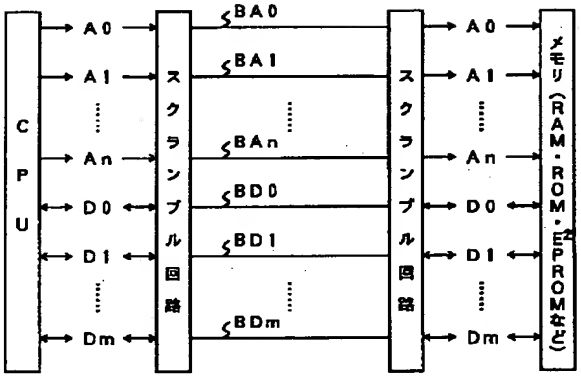
【図２】


10
11
BD0
BD1
60
タイミング制御回路
I/O-0
CPU
I/O-1
T00
T11
T01
T10
31
30
ROM
50
41
40
E²PROM
21
20
RAM

【図３】


CLK
(CPUからのクロック)
D
Q
O
ラッチ信号

【図４】


CPU
A0
A1
An
D0
D1
Dm
スクランブル回路
BA0
BA1
BAn
BD0
BD1
BDm
スクランブル回路
メモリ(RAM・ROM・EPROMなど)